

A METHOD OF ELLIPTIC CURVE ENCRYPTION

ABSTRACT OF THE DISCLOSURE

A method of elliptic curve encryption includes, (a) selecting an elliptic curve E_p (a,b) of the form $y^2 = x^3 + ax + b \pmod{p}$ wherein a and b are non-negative integers less than p satisfying the formula $4a^3 + 27b^2 \pmod{p}$ not equal to 0; (b) generating a large 160 bit random number by a method of concatenation of a number of smaller random numbers; (c) generating a well hidden point G (x,y) on the elliptic curve E_p (a,b) by scalar multiplication of a point B (x,y) on the elliptic curve with a large random integer which further includes the steps: (i) converting the large random integer into a series of powers of 2^{31} ; (ii) converting each coefficient of 2^{31} obtained from above step into a binary series; (iii) multiplication of binary series obtained from steps (i) and (ii) above with the point B (x,y) on the elliptic curve; (d) generating a private key n_A (of about ≥ 160 bit length); (e) generating a public key P_A (x,y) given by the formula $P_A(x,y) = (n_A \cdot G(x,y)) \pmod{p}$; (f) encrypting the input message MSG; (g) decrypting the ciphered text.